

VZCZCXYZ0001
OO RUEHWEB

DE RUEHKO #2895/01 1770953
ZNY SSSSS ZZH
O 260953Z JUN 07
FM AMEMBASSY TOKYO
TO RUEHC/SECSTATE WASHDC IMMEDIATE 4918
RUEKJCS/SECDEF WASHDC IMMEDIATE
INFO RUEAIIA/CIA WASHDC
RUEKJCS/CJCS WASHINGTON DC
RUENAAA/CNO WASHINGTON DC
RUYNAAAC/COMNAVFORJAPAN YOKOSUKA JA
RHHMHBA/COMPACFLT PEARL HARBOR HI
RHOVVKG/COMSEVENTHFLT
RUALSFJ/COMUSJAPAN YOKOTA AB JA
RUEAHQA/CSAF WASHINGTON DC
RHMFISS/DEPT OF HOMELAND SECURITY IA WASHINGTON DC
RHEFDIA/DIA WASHINGTON DC
RHMCSUU/FBI WASHDC
RHHMUNA/HQ USPACOM HONOLULU HI
RUEKJCS/JOINT STAFF WASHINGTON DC
RUEHKO/MLG TOKYO JA
RUYNAAQ/NAVCRRIMINVSERVFO FAREAST YOKOSUKA JA
RHEHAAA/NSC WASHDC
RHHJJPI/PACOM IDHS HONOLULU HI
RUENAAA/SECNAV WASHINGTON DC
RUEHKO/USDAO TOKYO JA
RUALSFJ/USFJ DIA REP YOKOTA AB JA

S E C R E T TOKYO 002895

SIPDIS

SIPDIS
NOFORN

OSD FOR APSA SHINN/SEDNEY/HILL/BASALLA; COMUSJAPAN FOR
J00/J2/J3/J5

E.O. 12958: DECL: 06/24/2017

TAGS: [PREL](#) [MARR](#) [PINR](#) [PGOV](#) [JA](#)

SUBJECT: INFORMATION SECURITY: AN ALLIANCE PRIORITY

Classified By: Ambassador J. Thomas Schieffer; Reasons: 1.4 (b/d)

¶1. (S) Summary: In tandem with the deepening of our bilateral alliance, the amount of information -- diplomatic, technical, intelligence, and operational -- provided to Japan has necessarily expanded exponentially over the past decade. Our ability to maintain momentum on information sharing, however, has been challenged by a series of unauthorized disclosures of classified information, including highly sensitive Aegis technical data. The Aegis case in particular has revealed serious gaps in Japan's structures for protecting classified information and conducting counter-intelligence investigations. Interventions by senior U.S. officials have alerted Japanese leaders to the extent of the problem. It is crucial that the U.S. government follow-up now by laying out a detailed roadmap to enhance Japan's ability to protect information. To ensure that this process remains credible, there needs to be a clear inter-agency message that future information sharing will be contingent on Japanese progress in correcting institutional and legal shortfalls. End Summary.

The Stakes

¶2. (S) The transformation of the U.S.-Japan Alliance over the past ten years has fundamentally altered the requirements for sharing information with Japan. As Japan has taken on new responsibilities within the alliance, such as providing enhanced operational support for U.S. forces and engaging in deeper cooperation on ballistic missile defense (BMD), there has been a corresponding need for greater information sharing. Providing Japan with sensitive diplomatic, technical, intelligence, and operational data is

fundamentally in the U.S. national interests. This information is used to protect our forces from current threats and to plan effectively for future regional contingencies. As Japan accepts a more active role within the alliance, equipping the Self-Defense Forces (SDF) with our most advanced systems will enhance our deterrent capability in the region and improve interoperability. In coming years, we expect information sharing related to BMD to contribute directly to the defense of the U.S. homeland.

The Challenge

¶3. (S) The fact that effective information sharing is so crucial to our own interests makes the recent disclosure of classified data so serious. A certain amount of unauthorized disclosures is inevitable in any country -- some people will leak for monetary, ideological, or simply "vanity" reasons. Recent incidents in Japan, however, suggest that the problem is more systemic, both in terms of Japan's structures for protecting information, and in terms of Japan's lack of appreciation for the counterintelligence problem it faces. Over the past year, we have seen damaging disclosures of intelligence data related to the DPRK's July 2006 missile launches, discussions in the press on sensitive bilateral planning activities, and the loss of operational data from laptop computers via commercial internet file sharing services.

¶4. (S) The most troubling recent episode relates to classified Aegis operational data found in the home of an uncleared Maritime Self-Defense Force (MSDF) member in January whose spouse is a PRC citizen found to be residing illegally in Japan. While a technical assessment of impact of the data compromise is still ongoing, initial analyses suggest that the information, if obtained by potential adversaries, might undermine the defenses of both U.S., Japanese, and other allied Aegis-equipped vessels. The U.S. government has registered our concerns about the case at senior Japanese political levels. This has resulted in Japan taking policy-level steps to assuage our concerns, including by committing to participate in a Bilateral Information Assurance Task Force (BIATF).

¶5. (S) High-level commitments of cooperation notwithstanding, the actions of Japanese agencies involved in the Aegis investigation have deepened longer term concerns over the Japanese government's ability to conduct effective counter-intelligence (CI) operations and investigations. Although the National Police Agency (NPA) has the stated lead on CI investigations, the MSDF and Kanagawa Prefectural Police (KPP) have been involved in the Aegis case. Both the MSDF and NPA have held back cooperation with U.S. and other Japanese agencies involved in the case. For example, the MSDF, NPA and KPP have strongly resisted U.S. efforts to obtain full access to the original hard drive required for forensic analysis. The embassy is also frequently in the position of learning new details about the investigation from leaks that appear in the press, rather than directly from Japanese officials. From what has been shared, it appears that the NPA is focused on achieving the quickest possible resolution to the case at the expense of establishing whether the data was obtained by potentially hostile governments.

Assessing the Problem

¶6. (S) The MSDF Aegis disclosure and problematic response are symptomatic of broader weaknesses in Japan's information assurance structure. Among the more serious challenges in fixing this structure are:

-- The absence of an information security culture: The Aegis case demonstrates that new laws and procedures alone are not enough to safeguard sensitive bilateral information in Japan. Classified information handled by the Ministry of Defense (MOD) and SDF personnel is covered by the Defense Secrets Act, which mandates strict penalties for unauthorized

disclosure; MOD also has a relatively robust process for background and security investigations, particularly for those with routine access to intelligence information. Despite these rules, MOD and SDF personnel are regularly the source of the most serious leaks of classified U.S. information. In many cases, media leaks are also sourced back to either senior officials seeking advantage over other agencies in the budget process or "vanity" leaks by mid-ranking officials looking to impress journalists.

-- Weak OpSec training/practices: The Aegis case and recent series of disclosures via internet file sharing programs suggest a pattern of poor electronic information security. The existence of an ongoing military officer/journalist exchange programs between a major daily newspaper (Sankei) and the SDF also illustrates a broader naivety about the CI threat and lack of concern for OpSec.

-- Lack of common security clearance system: There is no common standard background investigation or clearance system across the Japanese government. The deficiency exacerbates the stovepiping of information and leads to inconsistent screening for sensitive positions.

-- Uncoordinated CI structure: The Cabinet Office, MOD, and SDF components lack independent CI structures, leaving CI responsibilities to the Public Security Information Agency (PSIA) and the NPA. While the PSIA actively cooperates with U.S. counterparts on CI-related activities, it lacks the resources and authority to conduct CI investigations. For its part, the NPA works poorly with Japanese and U.S. national security agencies when a case involves potential prosecution. The NPA's effectiveness on CI is further limited by the nature of its relationships with local police departments. While local police departments nominally report to NPA, in reality NPA exerts little control over the actual conduct of an investigation. Additionally, there is no framework for local police to handle classified information they may come across during an investigation.

Charting a Way Forward

17. (S) Recent interventions on the Information Assurance issue by the Secretaries of State and Defense, the Director for National Intelligence (DNI), and Chief of Naval Operations (CNO) have succeeded in alerting Japan's political leadership to the seriousness with which the U.S. government views the problem. Fixing the problem, however, will take a sustained effort that involves all U.S. agencies engaged in managing the alliance. Delivering a consistent inter-agency message is a pre-requisite. Japanese agencies will try to resist change by waiting out the current Japanese political leadership and attempting to maintain a business-as-usual relationship with their U.S. counterparts.

18. (S) It will also be important for the inter-agency community to agree on both potential rewards and disincentives to ensure that Japan follows through on its information assurance commitments. The first step will be to define what leverage exists to encourage Japanese cooperation. We must convince Japan that a compromise of information by Japan is not a Japanese problem alone, but rather an alliance problem that undermines the security of both our countries. On the incentive side, we should look for training opportunities and bilateral structures that will build good practices. Finalizing a General Security of Military Information Agreement (GSOMIA) is a good first step towards creating a common system to protect sensitive data, that institutionalizes access, transparency, and accountability.

19. (S) As far as negative pressure points, we need to carefully weigh the costs and benefits of any decision to curtail ongoing or potential future information exchange initiatives. Much of what we are doing now is critical to our own national security. Upgrading Japan's Aegis fleet with SM-3 missiles, for example, will contribute directly to

the defense of our forces in the region. In contrast, although there is benefit to U.S. forces of developing an SM-3 missile maintenance facility in Japan, the Japanese political interest in such a facility may make our decision on whether to proceed a useful source of leverage to galvanize Japanese political leadership attention. Japan's proposal at the May 1, 2007 Security Consultative Committee (2 2) for a comprehensive information sharing roadmap is another possible source of leverage.

Looking to the End State

¶10. (S) In our own internal discussions and in our bilateral interactions with Japan, it is important to emphasize that the ultimate objective is to create a sound bilateral structure through which we can further deepen our information sharing relationship with Japan. Given the strategic challenges that the United States and Japan face in this part of the world, it is critical to keep moving ahead on transforming our alliance with Japan. There is no inherent reason why Japan cannot adopt the systems to protect sensitive data that partners like the United Kingdom and Australia maintain. It will require a sustained, coordinated inter-agency effort on the part of both Japan and the United States to move our alliance to that level of cooperation.
schieffer